

绪论
(第一章)

差分隐私和强化学习
定义及理论基础
(第二章)

原始数据保隐私聚合技术
(第三章)

标准化数据集产权保护技术
(第四章)

模型超参数泄漏风险评估技术
(第五章)

数据流通

总结与展望
(第六章)